

information security consulting

Consulting - Investigation - Training

information security consulting • michael krausz • mcse • csi • isoc
cumberlandstrasse 63/2c • a-1140 vienna, austria
tel +43 1 253 1000 • fax +43 1 253 1009 • **24h hotline +43 676 3 133 144**
email office@i-s-c.co.at • <http://www.i-s-c.co.at>

International Services Catalog

Navigating the Security Landscape from Takeoff to Landing



Introduction

Information security consulting (i.s.c.) founded in 1998, is active in three major areas supporting customers with strategic and tactical security services: **consulting, investigation** and **training**.

Consulting services cover a broad, yet carefully selected, range of services established successfully over the years, ranging from general purpose security consulting and CxO support services to highly specialized advice on audit matters (auditing customers as well as supporting customers in a contractual, regulatory or other certification audit) and entire multi-year projects devoted to getting or retaining ISO 27001 or PCI certification. Also covered are related standards such as the German Baseline Protection Manual or local national standards.

The **investigation** branch specializes in supporting a customer during or in the aftermath of any serious criminal or otherwise illegal action (e.g., civil law, business law) of which the customer was a victim. Scenarios include corporate embezzlement, fraud, money laundering, data theft and data leakages, DDoS blackmailing, trade in customer data, unfair competition, online and offline defamation, as well as physical threats. Our IT forensics unit operates as an auxiliary unit in this branch. i.s.c. has four Rapid Response Deployment Teams (RRDT) on 24hr duty to assure that a customer can be assisted in the following areas: personnel protection and evacuation, physical and IT-based eavesdropping, fraud (accounting fraud), and cybercrime. RRDTs services can be provided on a subscription or ad-hoc basis.

The **training** branch specializes in offering customized training, from individual sessions or programs to the setting up of entire academic training programs in the fields of security awareness, foundations of information and IT security, IT forensics and a limited set of standardized classes as described later in this document.

i.s.c. has always been at the forefront of the industry and has successfully executed over 400 projects since 1998. We have saved customers from legal damages in excess of EUR 25 million through our forensic services.

Should you have any questions or a general inquiry, please feel free to contact us anytime; should you face a serious security situation feel free to contact our 24h hotline to arrange first-response proceedings.

i.s.c. – information security. delivered.

Service Directory – Consulting

- Strategic CIO, CISO, CSO or IT-Security Director/Manager services
 - Studies, delivery of lines of arguments for in-house discussions
 - Developing short, medium and long term strategies or supporting their development
 - Providing confidential review and coaching or sparring services
- Governance, Risk, and Compliance consulting with a focus on IT and the relationship between IT GRC and corporate GRC topics
- Confidential CIO, CISO, CSO support
- Security reviews and audits to identify pain points in the IT, physical and human security sphere using our proven Comprehensive Security Check service product
- Drafting and roll-out of policies and procedures; development of policy frameworks
- ISO 27001 and PCI certification support projects (Certification Assistance Programs)
- Information security and IT security risk analysis
- Business risk analysis considering the relationship between information security and business risks
- Audits and reviews of information security management systems
- Systemic security audits of
 - IT architectures
 - IT systems (any kind of Windows or Unix based system, z/OS; other systems on request)
 - Network architecture and firewall reviews
 - VoIP telephony systems
- Penetration testing of web applications and network perimeters
- Web application security auditing
- Implementation of secure software development processes
- Business continuity management and planning
 - Drafting BCM and BCP frameworks
 - Drafting and testing of business continuity, business operations continuity and IT-service level continuity plans
- Drafting and deployment of security awareness trainings (such as the yearly trainings required by PCI) or entire security awareness programs.

Service Directory – Investigation and Evidence Acquisition

- **Emergency support through Rapid Response Deployment Teams (RRDT):**
 - RRDT Alpha
 - Personnel emergencies including evacuation from crisis areas
 - Preventing and dealing with workplace violence
 - CxO and key personnel travel protection services
 - RRDT Beta
 - Detection and removal of physical and IT-based eavesdropping devices
 - RRDT Gamma
 - Fraud and embezzlement
 - Forensic accounting
 - RRDT Delta
 - Strategic guidance in cases of information and IT security breaches
 - Strategic guidance in cases of white-collar crime in connection with cybercrime
 - Case assessments, damage containment measures
 - Execution of operations to identify perpetrators
 - RRDT services can be provided on a subscription or ad-hoc basis
- Strategic guidance and tactical support to acquire and provide evidence for later use in court proceedings or other strategic use
- Evaluation of incidents including damage assessment, damage propagation and damage containment
- Strategic guidance in relation to any crime or other illegal activity affecting the company
- Analysis of IT or information security breaches in high confidentiality environments

Service Directory – Training

- **Standardized Training Classes:**
 - ***Fraud in the IT Department*** – Prevention and Detection, offered as 1-day or 2-day training
 - ***Crime in the IT Department*** – Definition, Prevention, Detection, offered as 1-day or 2-day training
 - ***How to achieve ISO 27001 Certification*** – Overview and critical points, 1-day training
 - ***How to Achieve PCI Certification*** – Overview and critical points, 1-day training
 - ***How to Cope with Audits*** – Dealing with special audit situations, 1-day training
 - ***How to Set Up a Security Awareness Program*** – 1-day training

These classes are available in extended versions. By customer request, content can be agreed upon, resulting in bespoke training.

- **Customized Training** is available on all items covered as consulting services to assure that a customer obtains a targeted know-how transfer. The purpose of such training is to enable the customer to execute a full project autonomously and achieve the most beneficial ratio of internal vs. external effort in the project.

Past examples include (non-exhaustive list):

- ***Drafting Business Continuity Plans*** – Methods and Tools
- ***Conducting Internal Information Security Audits***
- ***Determining Information Security Risk Levels***
- ***Risk Analysis According to ISO 27005***
- ***Setting Up an Accreditation Body According to ISO 27006***
- ***Breach Resolution Using ISO 27035***
- ***IT-Forensic Investigator Education & Training*** (2-year academic training program)